TEXOMA MEDICAL CENTER

PLEASE READ BEFORE SUBMITTING THE FORMS:

Instructions for Requesting Access to Texoma Medical Center Network/Information Systems.
Access should now be requested using the following link: (copy and paste into a browser if the link does not work.)
https://fs20.formsite.com/gstepp/2wei2nbcc8/index.html
The link is also available at www.texomamedicalcenter.net. Remote Access link is on at the bottom of the main page.

1. Agreement forms are still required and there are links for those on the new form. All added forms should be sent in PDF format. Agreement forms are also available on www.texomamedicalcenter.net under Remote Access menu located at the bottom of the main page.
2. All practices must submit a **"**Health Information Data Access Agreement**"** if there is not one on file. Periodic audits may require a new agreement. The form should be signed by the provider and use the name of the office as the "provider" in the form. This form is not required by individuals. Only one is needed for the office. Third party billing companies must complete the **"**Business Associate Agreement**"** document instead of the **"Health Information Data Access Agreement."**
3. Users may not share accounts. Each user must complete the required documents, have and use their own accounts. To access records under another person's access is a violation of UHS Policy and HIPAA.
4. Each user requesting access must also complete a **"Remote for Access Form for Texoma Medical Center"** from the above link. Be sure and complete the agreements with the access form. This form is sent automatically to TMC staff. Links for the additional forms are on the online form.
5. Each user requesting access must also complete and sign the **"**Information Security and Privacy Agreement**",** writing initials in each box. Agreement is void if one initial and a line is drawn through the rest is placed on form or they are typed.
6. The remote access form will be automatically sent to TMCREMOTEACCESS@THCS.ORG. Additional required forms should be sent to the same email and must be in PDF format.
7. Once access is granted, a designated representative of the office will receive the login information and is responsible for keeping TMC Information Systems Department informed when staff leave so access can be removed. If a user does not use their access for 30 days it is deactivated per UHS Corporate policy and deleted at 60 days. This could require submission of all new forms to reactivate access.
8. A user is responsible for keeping their login and password secure and will be required to change their password every 90 days. Logins cannot be shared.
9. Access will be completed 7-10 days from receipt of all accurately completed forms.
10. Access is restricted to business use. If the login is used to access personal or family accounts that are not patients of your clinic/company, access may be revoked.
11. For Cerner access, Microsoft Two-Factor authentication will be required. Details would be sent when access information is completed.
12. Most TMC applications are now using 2FA methods to be accessed remotely. The process may require the use of the user's cell phone to receive a code for authentication. The cell phone # is required to be completed on the access form.
13. Methods for 2FA are Microsoft Authenticator for TMC EMR (Cerner Fusion) and VIP Access to obtain a security code for others. Both applications are free and can be downloaded from the Apple or Google Play store. We recommend the app be installed on your cell phone.
14. Offices are responsible for providing their own IT support to work through any issues accessing the site or hardware requirements. Citrix is required to access Cerner and the correct version can be downloaded from the web site. See Citrix Remote Access Requirements. Other systems may have their own requirements and methods to access. The designated office representative will receive information once completed.